Übernahme von Objekten aus dem Novell Directory Service in das Active Directory

1. Wie wirken sich die Unterschiede zwischen Windows 2000 und Windows 2003 auf die Aufgabenstellung aus?

Unterschiede zwischen Windows 2000 Advanced Server und Windows 2003 Advanced Server

Veränderte GUI

Voreingestellte Sicherheitsrichtlinien

z.B.:

- Mindestpasswortlänge: 6 Zeichen
- Komplexitätsregeln eingeschaltet
- Kennworthistorie eingeschaltet

Standardmäßige SMB Signierung

Windows 2003 DC verwenden standardmäßig digital signierte SMB Kommunikation. Das betrifft freigegebene Ordner, freigegebene Drucker, einige administrative Funktionen und die Anmeldeauthentifikation.
Clients mit WfW, W95 ohne AD Client und NT 4.0 mit SP2 unterstützen keine SMB Signierung. Sie können sich standardmäßig nicht an Windows2003 DCs anmelden.

Adminpack 2003

Das Adminpack 2003 kann nur auf XP installiert werden.
Das Adminpack 2000 kann nicht zur Verwaltung von Windows 2003 Servern verwendet werden.

IIS 6.0 ist stark überarbeitet worden.

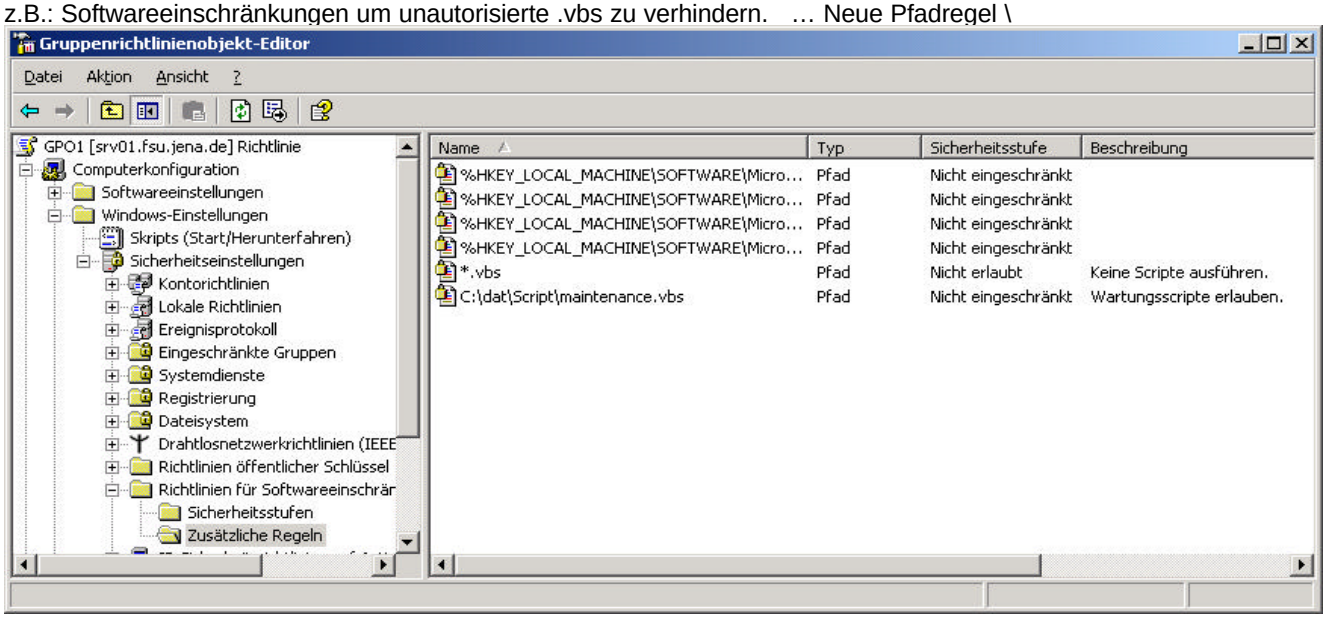
Siehe Installationsmenü.

Änderungen am Dateisystem

Von Windows 2000 kann nicht auf alle Windows 2003 Serververzeichnisse zugegriffen werden.

Erweiterte GPOs

z.B.: Softwareeinschränkungen um unautorisierte .vbs zu verhindern. … Neue Pfadregel \



Zusätzliche Lizenzkosten für Windows 2003 Server und Windows XP Clients, aus den oben genannten und weiteren Gründen, führten zu der Entscheidung, die Objektübernahme mit Windows 2000 zu erarbeiten.

2. Automatisierte Übernahme von Nutzern aus dem NDS in das AD

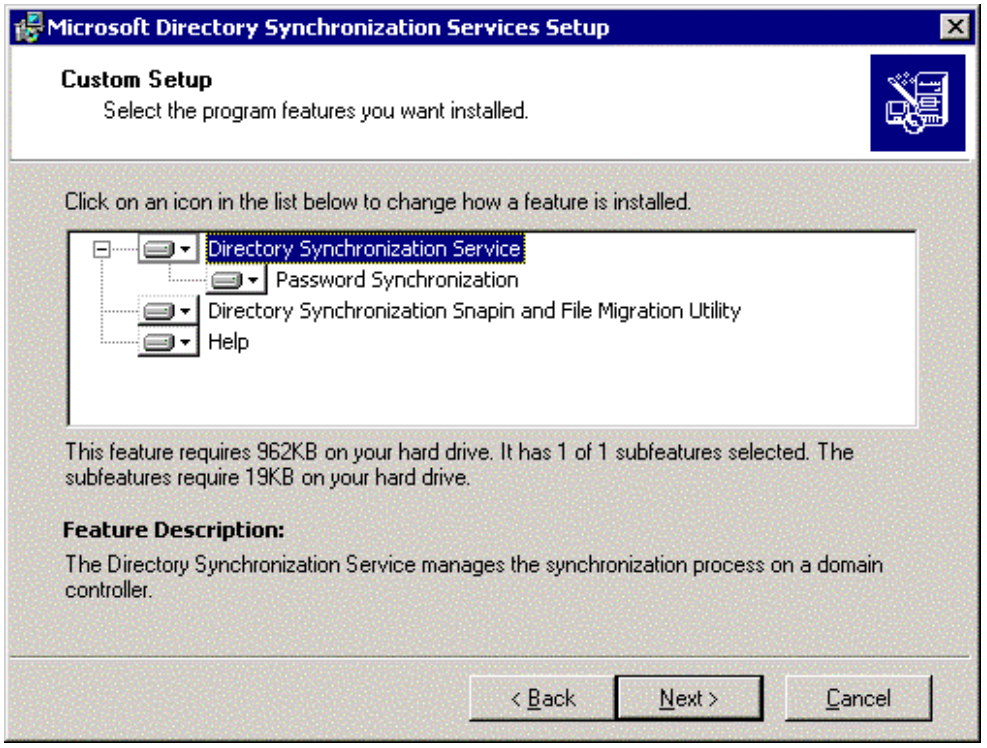
Lizenz- und Kostenlage

Das Tool Microsoft Services for Netware liegt in verschiedenen Versionen vor.

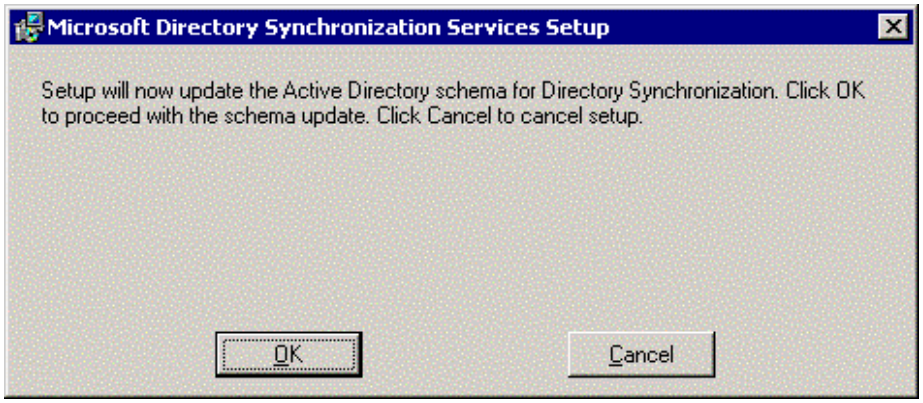
- Microsoft Services for Netware 5.02
  - o für Windows 2000
  - o für verschiedene Sprachversionen vorhanden, auch für deutsch
  - o Kostenpflichtig, letzter gefundener Preis: 149,- €.
  - o letztes Servicepack: Release 2

- Microsoft Services for Netware 5.03a
  - o für Windows 2003
  - o freeware, nur in englisch verfügbar
    - ▪ Läuft die englische Version auch auf deutschen Servern ohne Beanstandungen?

Installation des Microsoft Services for Netware 5.03a

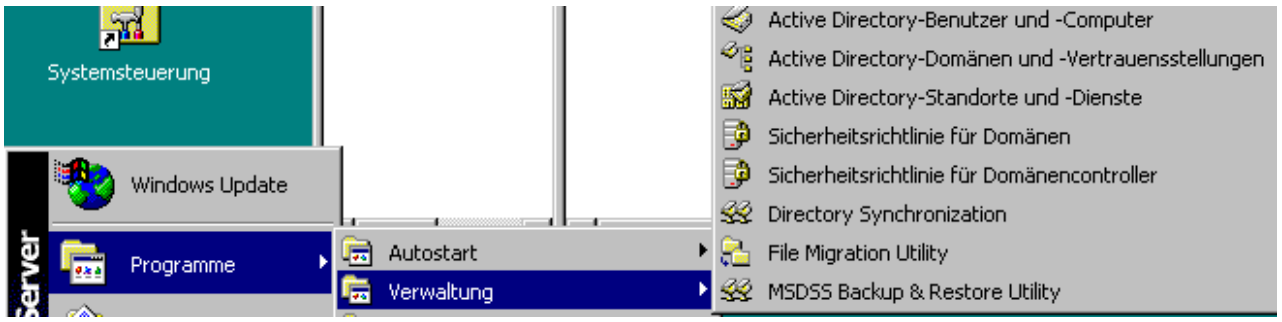


Achtung, eine Schemaänderung ist notwendig.

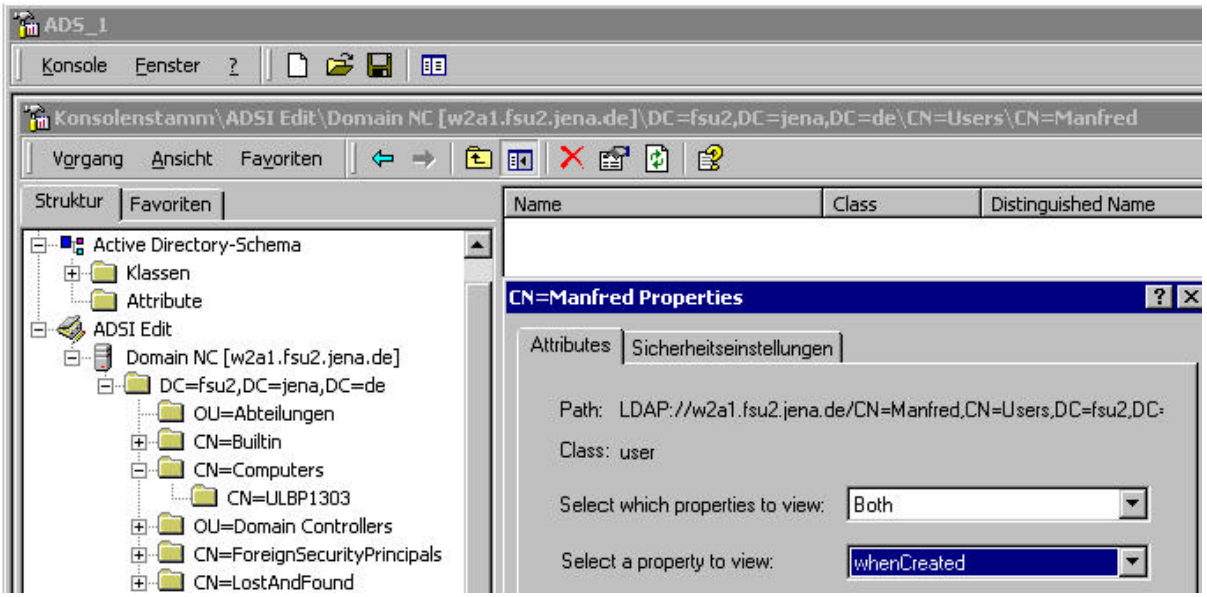


Nach der Installation stehen unter der Verwaltung folgende Tools zur Verfügung.

- Directory Synchronization
- File Migration Utility
- MSDSS Backup & Restore Utility



Die Schemaänderung kann mit dem ADSI Edit überprüft werden.

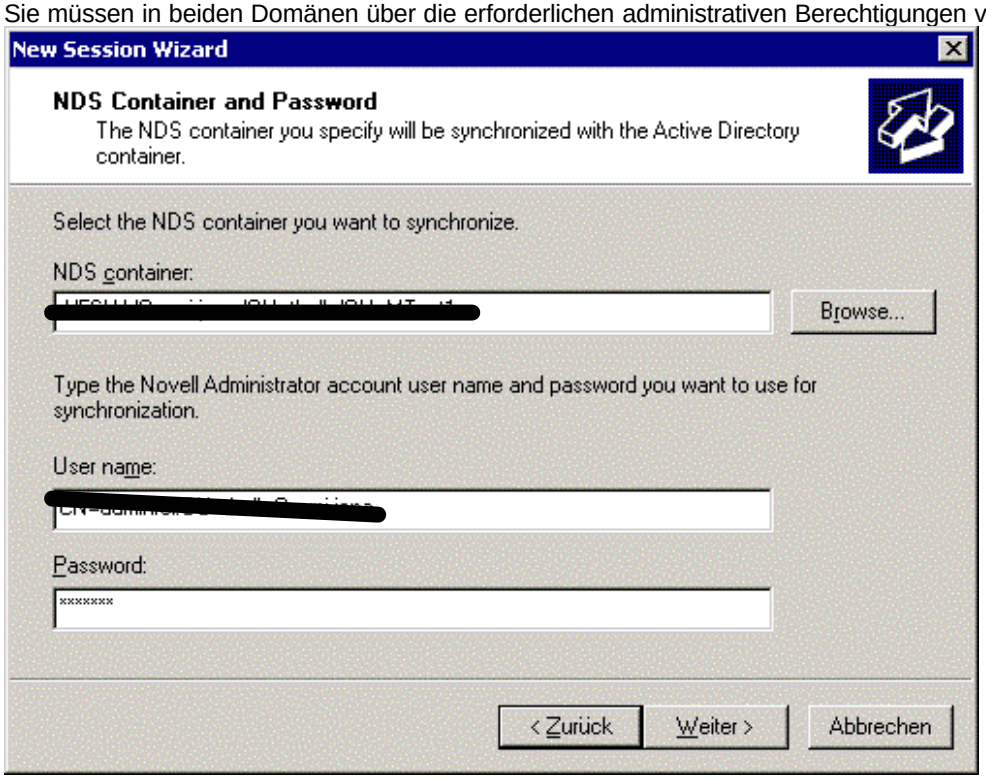


Test: Directory Synchronization Service

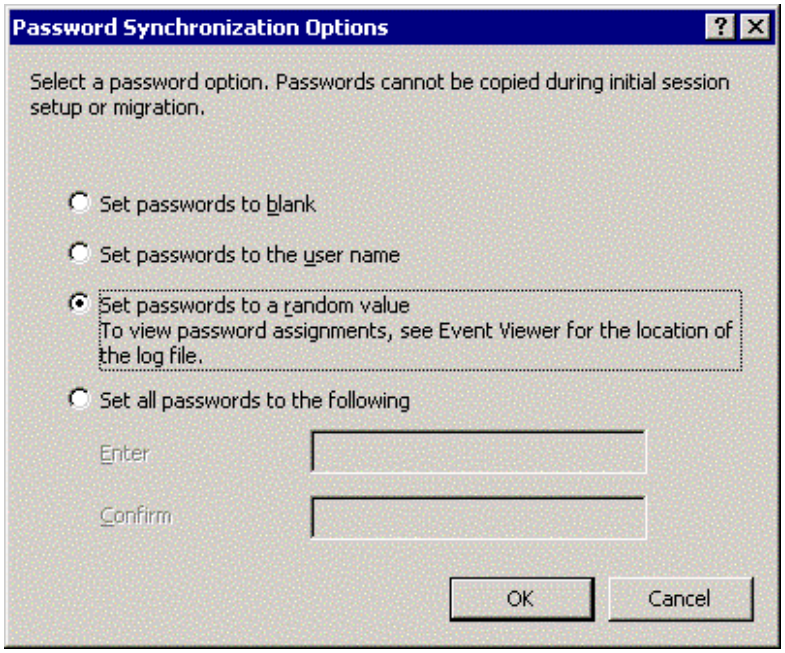
Zum Test wurde in der NDS eine untergeordnete OU mit verschiedenen Objekten angelegt.

Nach dem Aufruf des Directory Synchronization Tools werden Sie von einem Assistenten durch die notwendigen Arbeitsschritte geführt.

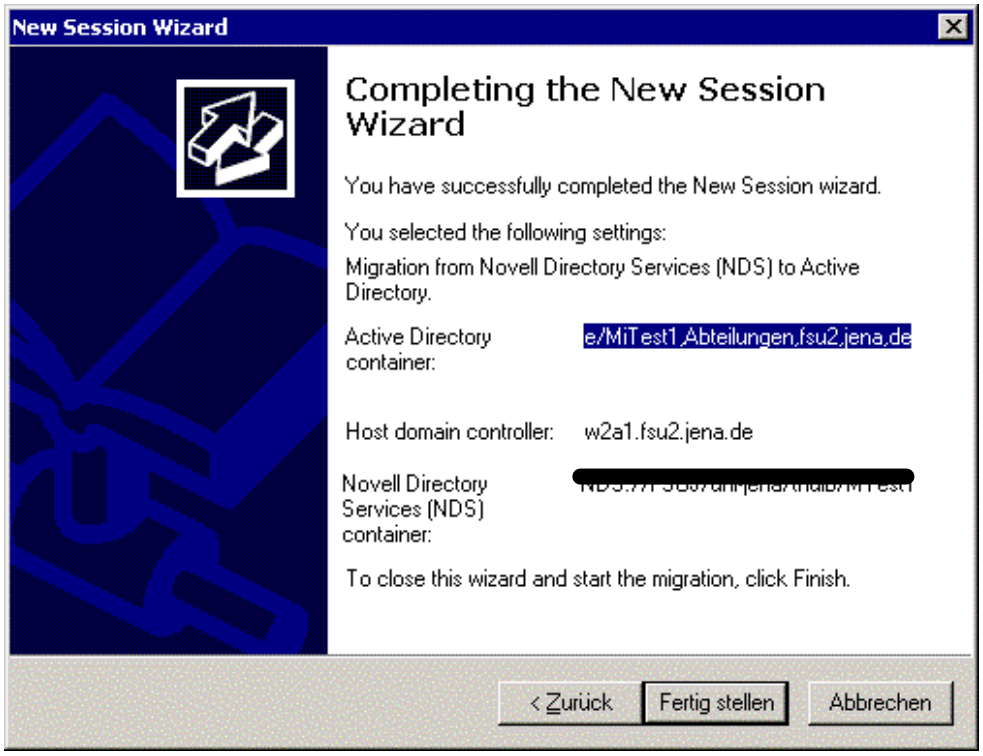
Sie müssen in beiden Domänen über die erforderlichen administrativen Berechtigungen verfügen.

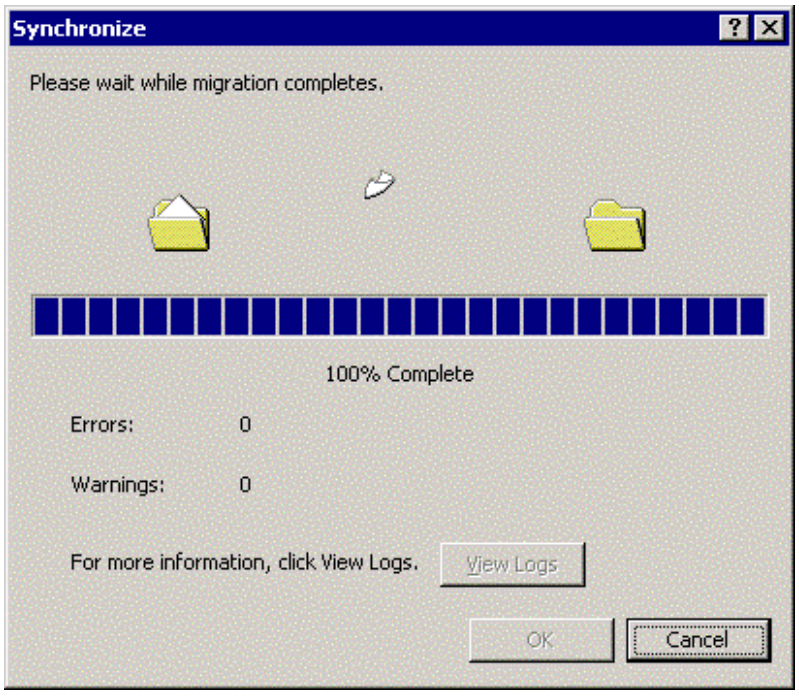


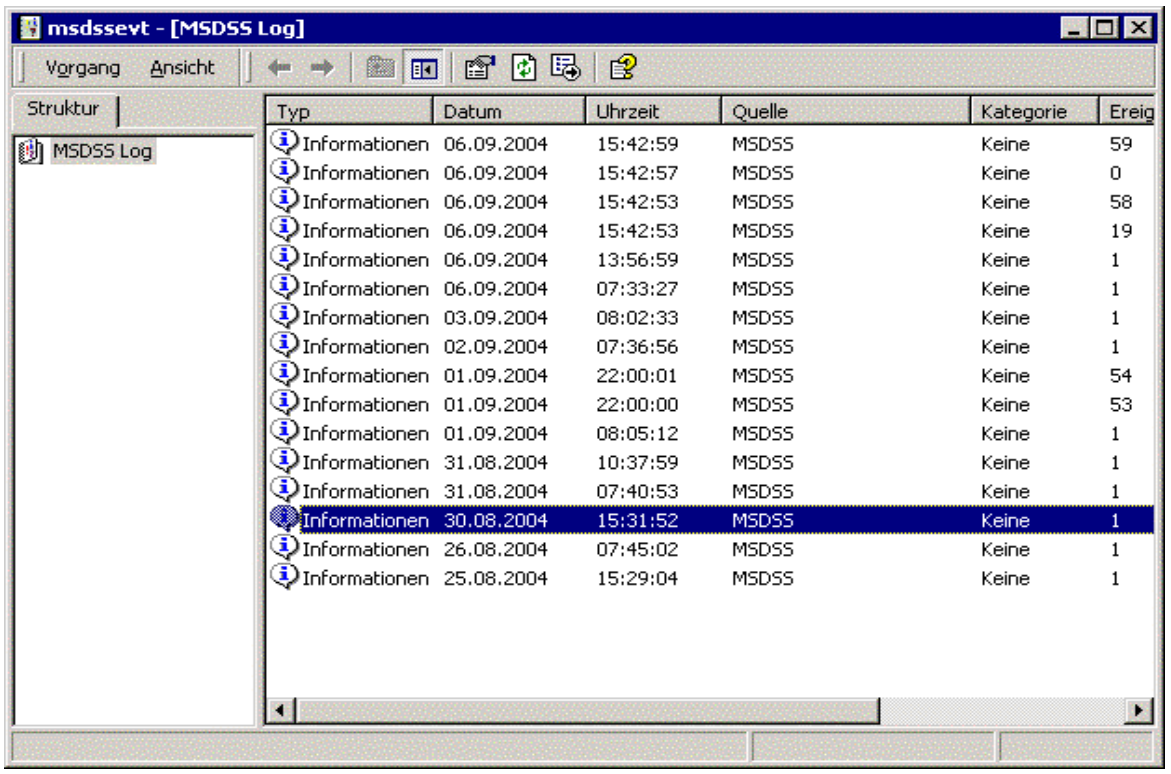
Leider wird das originale Passwort nicht mit übernommen, hier können die verschiedenen Übernahmeoptionen eingestellt werden.



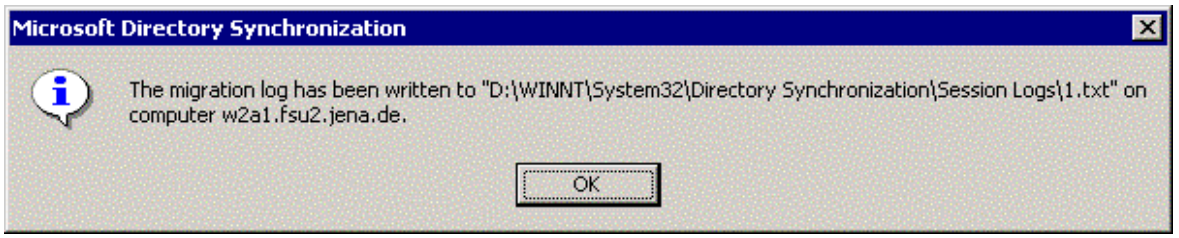
Am Ende des Assistenten können die Einstellungen noch einmal überprüft werden.



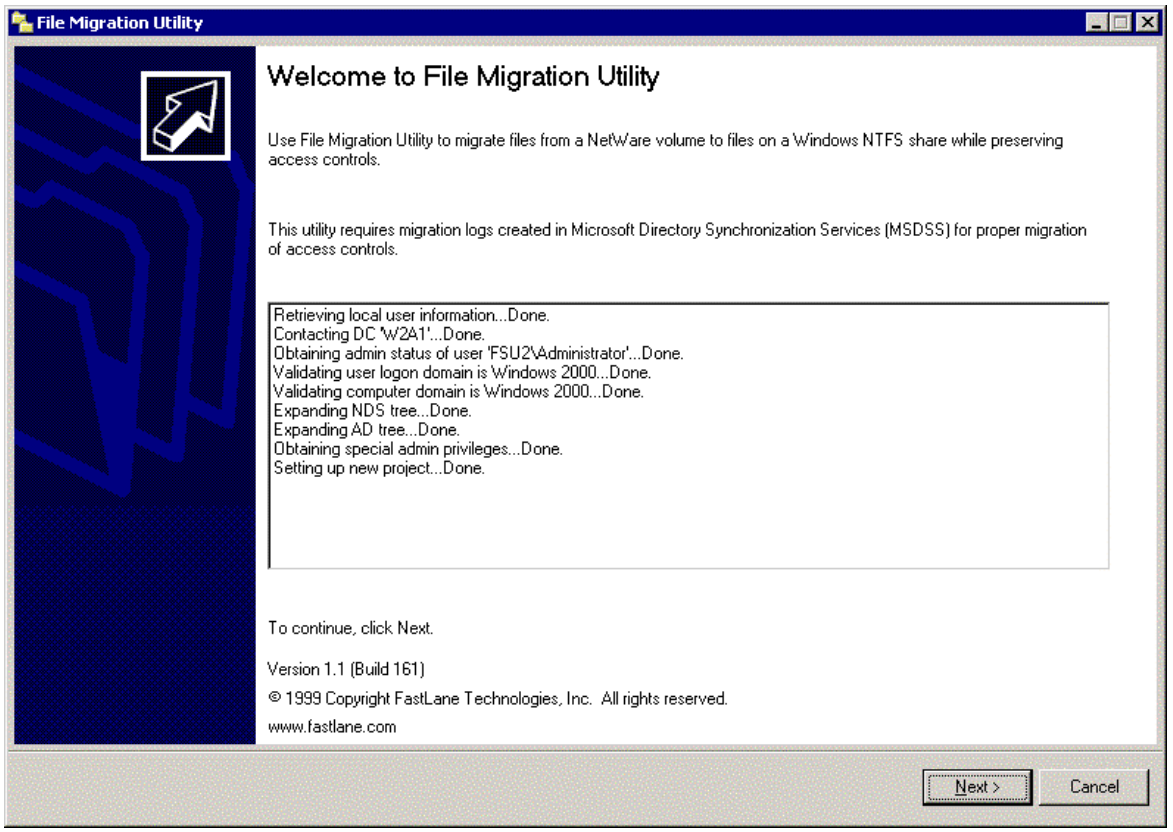


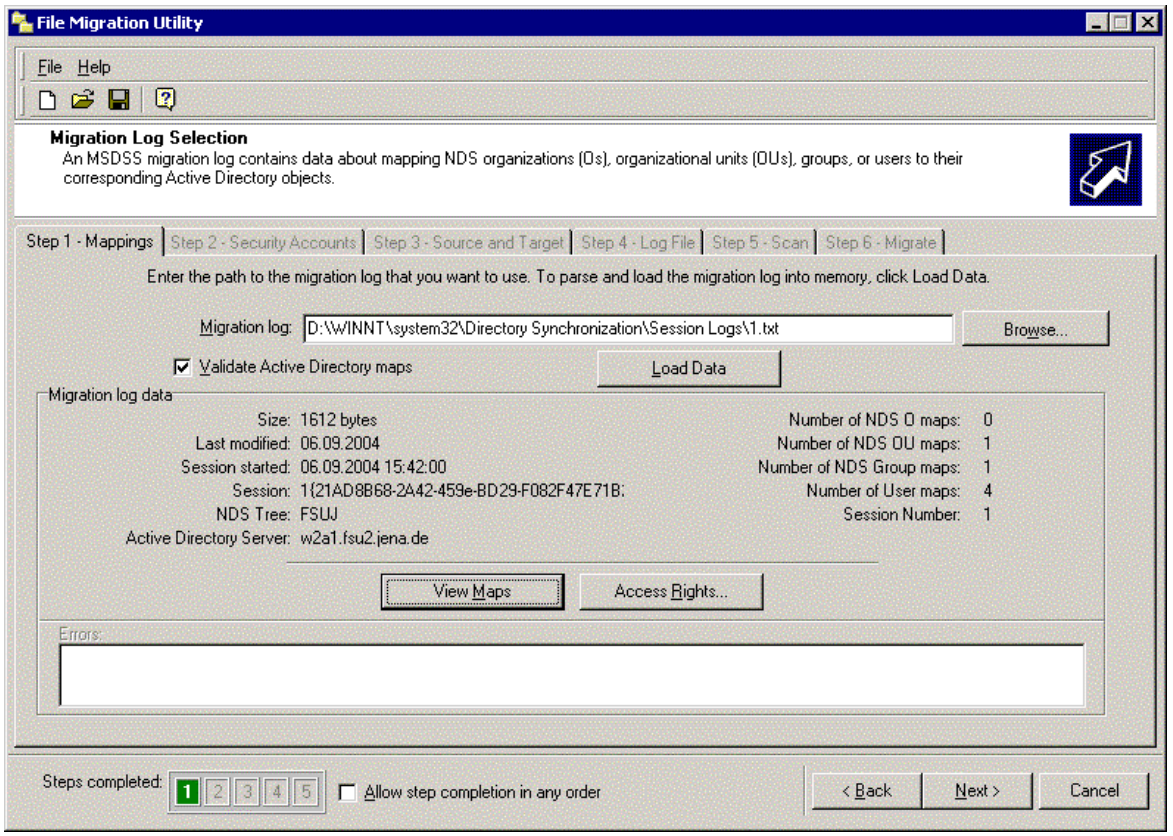


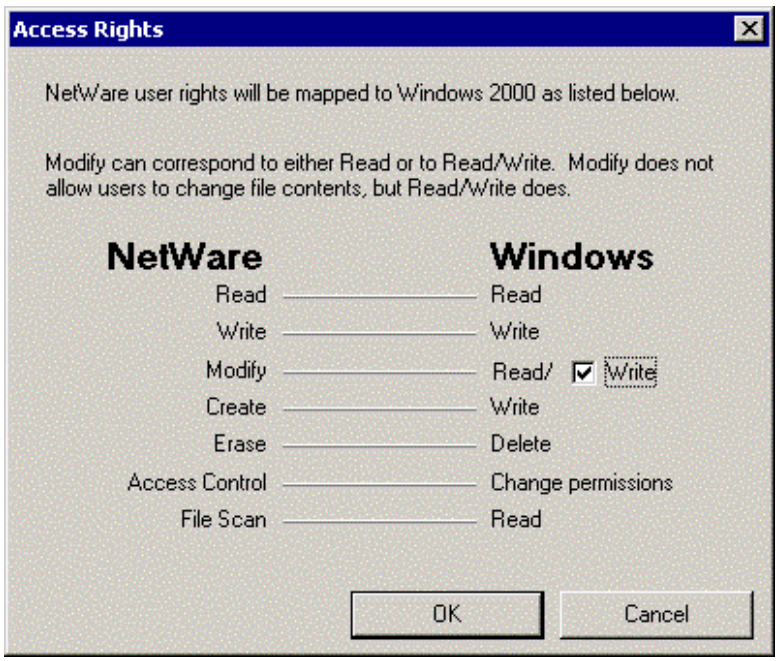
Das migration log wird für das File Migration Utility benötigt.



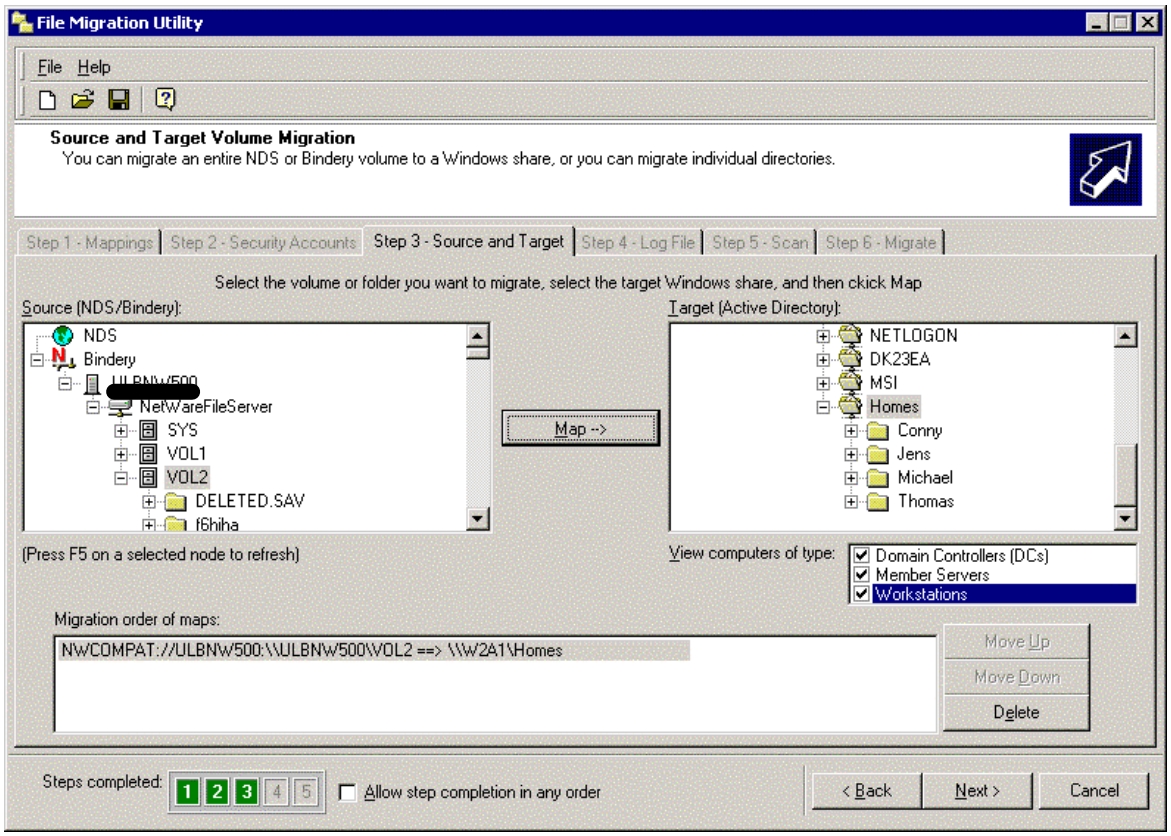
Test: File Migration Utility



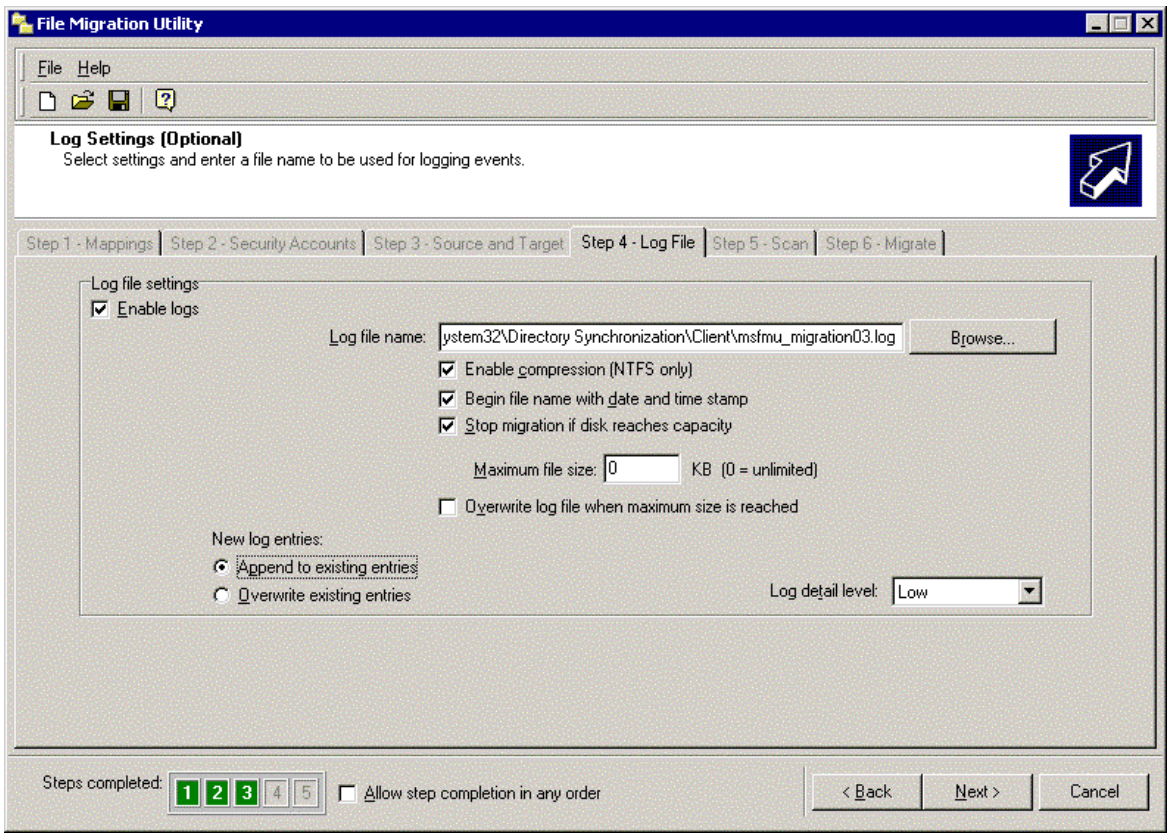


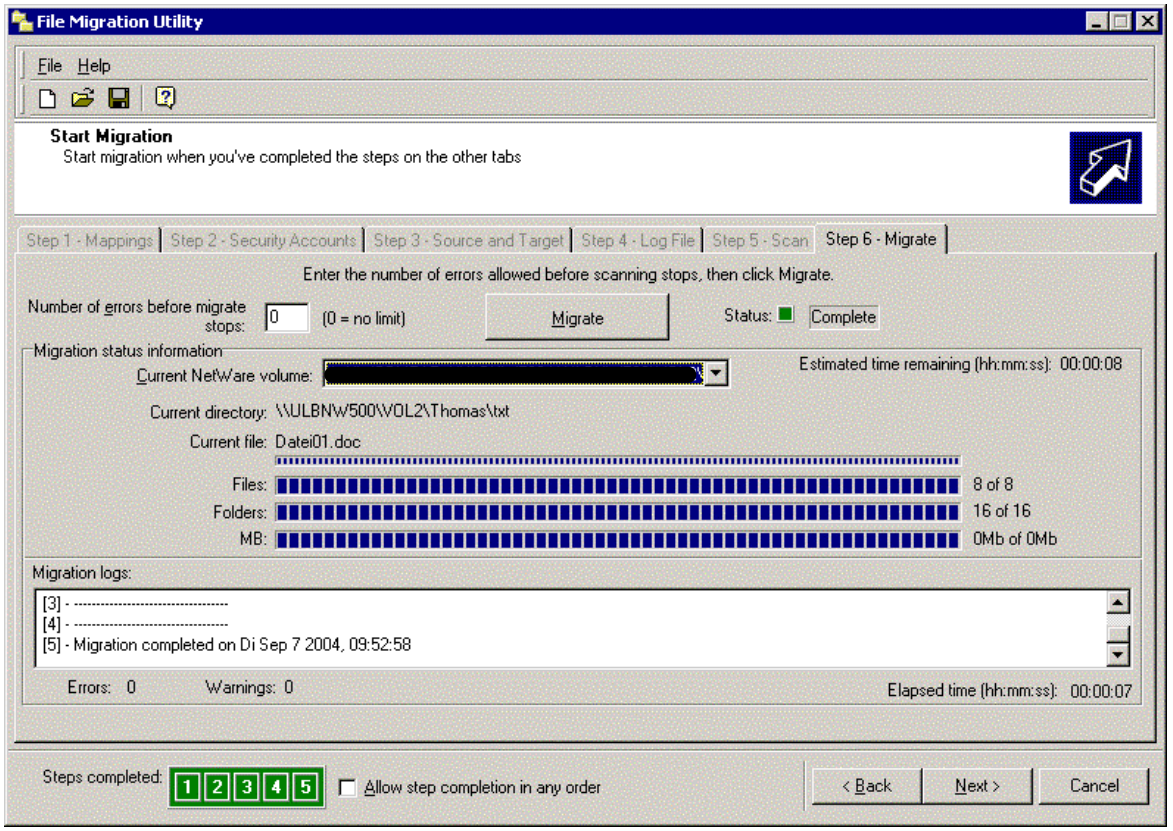


Im File Migration Utility gibt es die Möglichkeit das komplette Volume zu übernehmen.

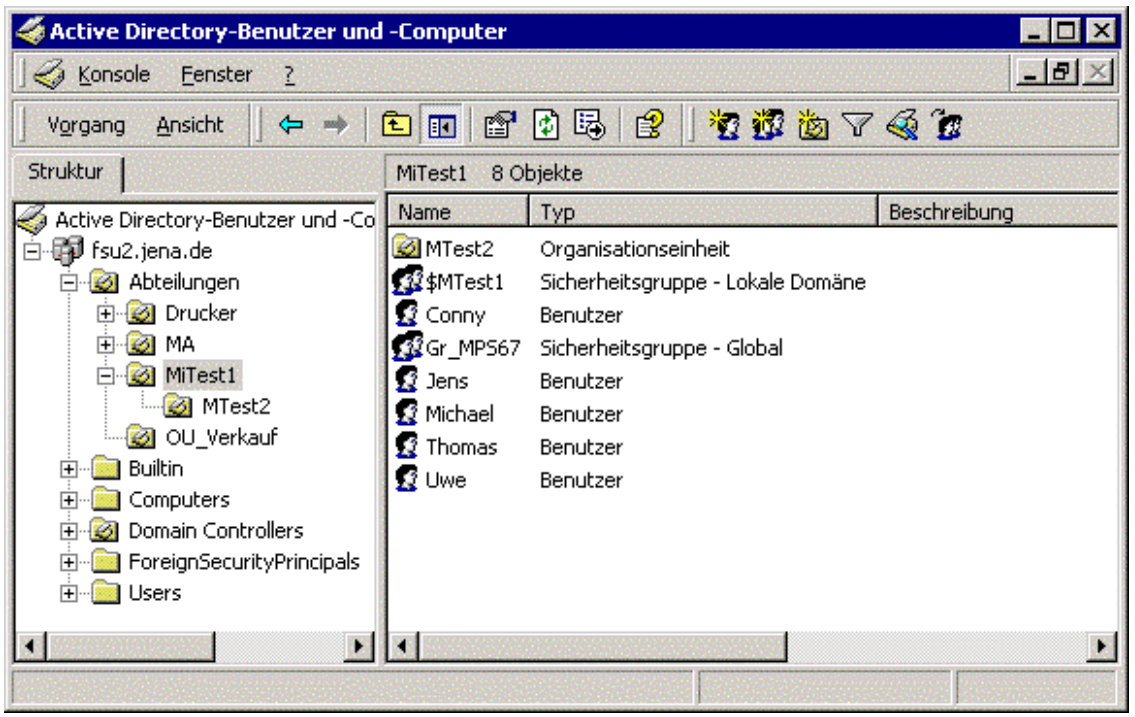


Zur Übung werden hier nur die Homelaufwerke der Testnutzer übernommen.





Den Arbeitsfortschritt und die Erfolgsanzeige bietet das letzte Fenster.



Gruppen und OUs werden richtig übernommen.

3. Automatisierte Übernahme von Nutzern aus dem NDS in das AD ohne Schemaänderungen

Grund: Vorhandene Directories sind Bestandteile übergeordneter Strukturen.

Die verfügbaren Tools erfordern aber eine Änderung des Schemas entweder in der Zieldomäne oder in der Quelldomäne.

Was kann die Lösung sein?

Eine Möglichkeit bietet hier die strukturübergreifende Migration. Dazu wurde eine Transferdomäne mit einer bidirektionalen Vertrauensstellung eingerichtet.

Das DNS der Transferdomäne muss folgende Einträge fehlerfrei übernehmen.

Diese Einträge werden vom Netlogon (Anmeldedienst) Dienst vorgenommen.

_tcp

Name	Typ	Daten
_gc	Dienstidentifzierung	[0][100][3268] servername.Domänenname.
_kerberos	Dienstidentifzierung	[0][100][88 servername.Domänenname.
_kpasswd	Dienstidentifzierung	[0][100][464] servername.Domänenname.
_ldap	Dienstidentifzierung	[0][100][389] servername.Domänenname.

_udp

Name	Typ	Daten
_kerberos	Dienstidentifzierung	[0][100][88] servername.Domänenname.
_kpasswd	Dienstidentifzierung	[0][100][464] servername.Domänenname.

Vertrauensstellungen zwischen Domänen unterschiedlicher forests einrichten

Diese Vertrauensstellung lässt sich mit netdom trust einrichten.

netdom trust Zieldomäne /domain:Quelldomäne /userD:admin /PasswordD:******* /userO:admin /PasswordO:******* /add /PasswordT:******* /verbose

Establishing a session with \\server
Reading LSA domain policy information
Establishing a session with \\server
Reading LSA domain policy information
Trust information for domain Domänenname
written to domain Domänenname
Trust information for domain Domänenname
written to domain Domänenname
Deleting the session with \\server
Deleting the session with \\server
The command completed successfully.

netdom query trust

Direction	Trusted\Trusting domain	Via domain	Status
<-	Domänenname		

The command completed successfully.

netdom query trust

Direction	Trusted\Trusting domain	Via domain	Status
<->	Domänenname		

The command completed successfully.

Die Erfolgskontrolle in der grafischen Oberfläche erfolgt unter dem Active Directory Domänen und Vertrauenstellungen.

Voraussetzung für die Nutzung von ADMT:

bidirektionale Vertrauensstellungen

Gruppen
Erstellen Sie in der Quelldomäne eine neue lokale Gruppe mit dem Namen Quelldomäne$$$.
Hinweis: Diese Gruppe darf keine Mitglieder enthalten.

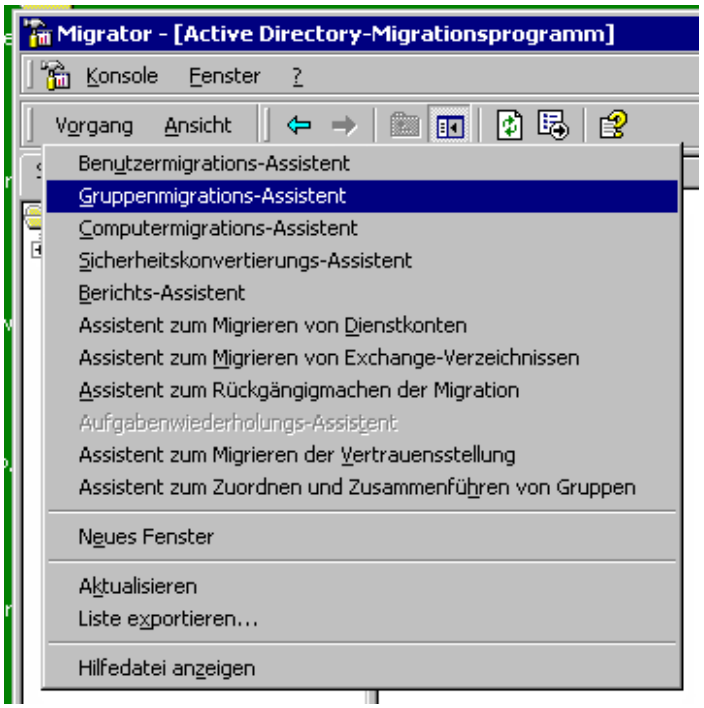
Überwachung
Aktivieren Sie die Überwachung für erfolgreiche bzw. fehlgeschlagene Benutzer- und Gruppenverwaltungsvorgänge in der Quelldomäne.
Aktivieren Sie die Überwachung für erfolgreiche bzw. fehlgeschlagene Überwachung der Kontenverwaltung in der Standarddomänencontroller-Richtlinie der Zieldomäne.

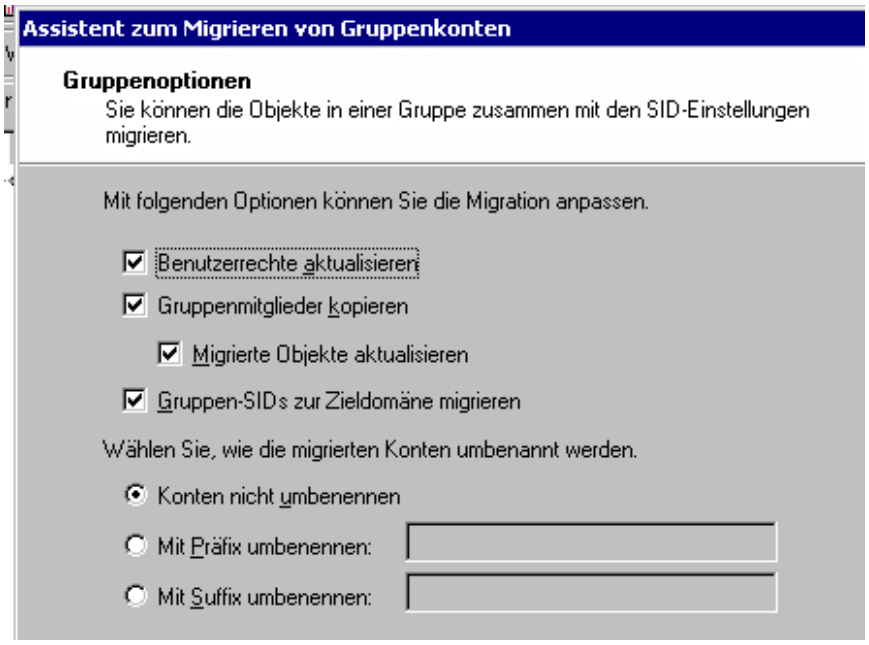
Registrierung
Fügen Sie auf dem PDC der Quelldomäne den Wert TcpipClientSupport:REG_DWORD:0x1 zu dem folgenden Registrierungsschlüssel hinzu:
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\LSA

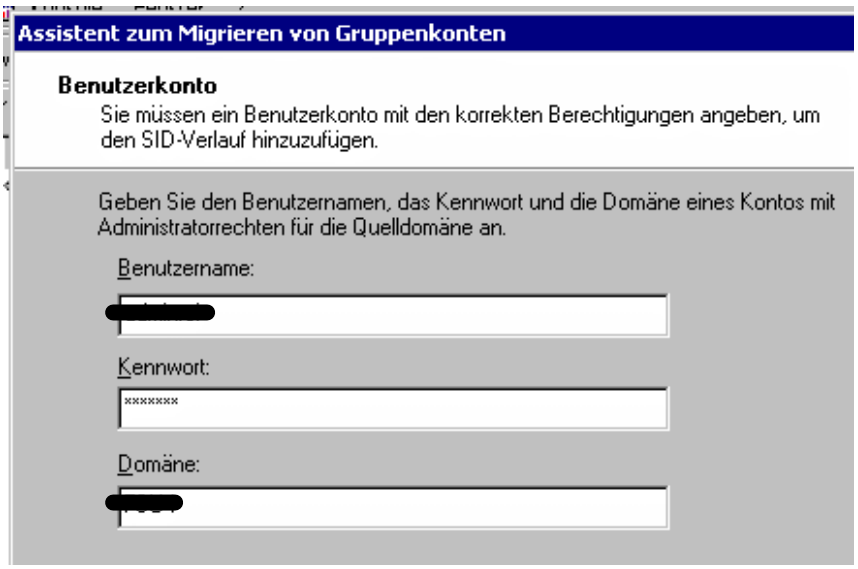
Administrative Freigaben
Auf dem Domänencontroller in der Zieldomäne, auf dem ADMT ausgeführt wird, sowie auf allen Computern, auf denen ein Agent ausgeführt werden muss, müssen administrative Freigaben vorhanden sein.

Benutzerrechte
Sie müssen sich auf dem Computer, auf dem ADMT ausgeführt wird, mit einem Konto mit den folgenden Berechtigungen anmelden:
Domänenadministrator-Berechtigungen für die Zieldomäne
Mitglied der Gruppe Administratoren in der Quelldomäne.
Administratorberechtigungen auf jedem zu migrierenden Computer.
Administratorberechtigungen auf jedem Computer mit zu konvertierender Sicherheit.
So werden Sie über die erforderlichen Berechtigungen verfügen, wenn Sie sich mit dem Konto "Quelldomäne\Administrator" bei dem PDC anzumelden, der FSMO-Funktionsinhaber in der Zieldomäne ist. Hierbei wird vorausgesetzt, dass die Gruppe "Quelldomäne\Domänenadministratoren" zur Gruppe Administratoren auf den jeweiligen Computern gehört.

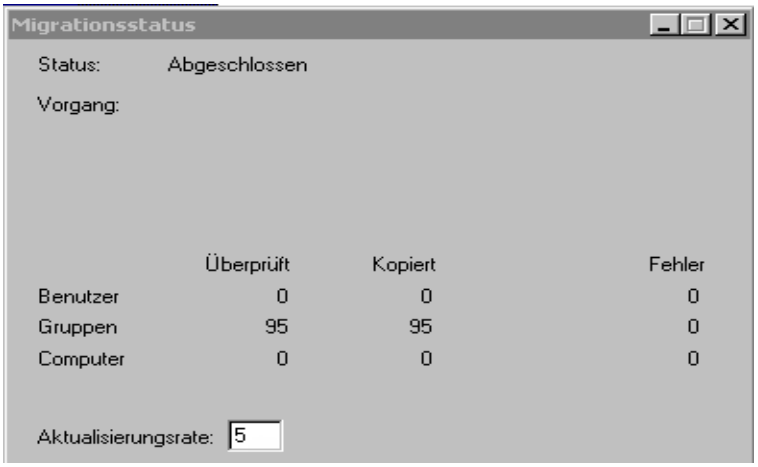
Ausführung des ADMT:







Neue Kennwortauslagerungsdatei:
C:\Programme\Active Directory Migration Tool\Logs\passwords.txt



Logdatei unter:

C:\Programme\Active Directory Migration Tool\Logs\

Damit wurden die Gruppen erfolgreich mit den SID Verläufen übernommen.

Rationelles zufügen von Nutzern zu einer Gruppe

'Usrtogrp.exe'

usrtogrp *filename*

Note

If you are manipulating a local group, UsrToGrp will also search trusted domains, so user accounts should be specified as "UserName", not "DomainName\UserName".

4. Zuweisung von Netzdruckern an Nutzer im AD auf Grund von Gruppenzugehörigkeiten

Wo ist das Problem?

Standardmäßig wirken GPOs im AD nur auf Mitglieder einer OU, nicht jedoch auf die Mitglieder einer Gruppe die sich in der OU befindet.

Das Problem ist im Netz bekannt und wird in verschiedenen Foren gefragt. Jedoch waren hier keine plausiblen Antworten zu finden.

Hier musste eine Technik angewendet werden, die beispielsweise administrative Gruppen von hinderlichen Beschränkungen durch Standard GPOs der Site oder Domäne freihalten soll. Dabei wird das Anwenden dieser GPOs auf diese Gruppenmitglieder verhindert. Diese Technologie musste praktisch umgekehrt werden.

Zur Lösung des Problems werden die GPOs der zutreffenden Gruppen auf Site- oder Domänenebene so gefiltert, dass die entsprechende GPO nur auf diese Nutzer zutrifft.

Voraussetzungen:

- Gruppen für Mitglieder gleicher Zugriffsrechte auf Netzwerkdrucker
- ein GPO für jede Gruppe
- Die vorgesehenen Netzwerkdrucker werden durch ein Startskript zugewiesen.
- Netzdrucker sind freigegeben

Weiterhin wurde die Möglichkeit geschaffen, Netzwerkdrucker, welche weder freigegeben noch im Verzeichnis veröffentlicht wurden, über GPOs bestimmten Computern zuzuordnen. Dies geschah auf der Grundlage der vorhandenen Vorarbeit der Netzadministratoren.